(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－161172

(43)公開日　平成７年(1995)６月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ１１Ｂ	23/28	Ｚ	7177－5Ｄ		
	23/30	Ｂ	7177－5Ｄ		
		Ｚ	7177－5Ｄ		

審査請求　未請求　請求項の数４　ＯＬ　（全 10 頁）

(21)出願番号　特願平5－304214

(22)出願日　平成５年(1993)12月３日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　井村　滋
東京都品川区北品川６丁目７番35号　ソニー株式会社内

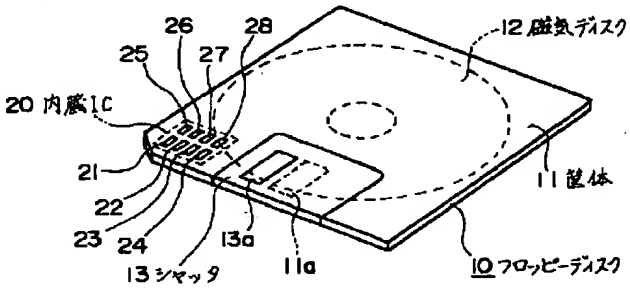
(74)代理人　弁理士　松隈　秀盛

(54)【発明の名称】　データ記録媒体

(57)【要約】

【目的】　各種データをディスク，テープ等の記録媒体に記録させる場合に、セキュリティ性が高く且つ使い勝手の良い記録ができるようにする。

【構成】　データが記録される記録媒体１２を筐体１１に収納させ、この筐体１１の所定箇所にＩＣ２０を取付けてなるデータ記録媒体において、記録媒体１２に起動プログラムと暗号化されたデータとを記録させ、記録データの暗号化プログラムと暗証番号のデータとをＩＣ２０内のメモリに記憶させ、記録されたデータを読出す場合又は記録媒体１２にデータを書込む場合に、入力された暗証番号をＩＣ２０に供給させて、このＩＣ２０内のメモリに記憶された暗証番号と演算手段が照合させ、暗証番号が一致した場合には、ＩＣ２０内のメモリに記憶された暗号化プログラムに従って、記録媒体１２に記録された暗号化されたデータの復号又は記録媒体１２に記録するデータの暗号化をできるようにした。



フロッピーディスクの構成

【特許請求の範囲】
【請求項１】　所定の方法でデータが記録される記録媒体を所定の筐体に収納させ、該筐体の所定箇所にメモリと演算手段とを有するＩＣを取付けてなるデータ記録媒体において、
上記記録媒体に起動プログラムと暗号化されたデータとを記録させ、上記暗号化されたデータの暗号化プログラムと暗証番号のデータとを上記ＩＣ内のメモリに記憶させ、
上記記録媒体に記録されたデータを読出す場合又は上記記録媒体にデータを書込む場合に、入力された暗証番号を上記ＩＣに供給させて、このＩＣ内のメモリに記憶された暗証番号と演算手段が照合させ、暗証番号が一致した場合には、ＩＣ内のメモリに記憶された暗号化プログラムに従って、上記記録媒体に記録された暗号化されたデータの復号又は上記記録媒体に記録するデータの暗号化をできるようにしたデータ記録媒体。
【請求項２】　ＩＣ内での暗証番号の照合で、予め定めた所定回連続して不一致を検出したとき、以後の照合で暗証番号が一致しても暗号化プログラムを出力させないブロックを行うようにした請求項１記載のデータ記録媒体。
【請求項３】　予め定めた所定回連続して不一致を検出してブロックされた状態で、上記暗証番号とは別に設定された暗証番号を入力させることで、ブロックの解除を行うようにした請求項２記載のデータ記録媒体。
【請求項４】　ＩＣ内のメモリに付加情報を記憶させるようにした請求項１記載のデータ記録媒体。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、フロッピーディスク等の磁気ディスク，光磁気ディスク，光ディスク，磁気テープなどの各種記録媒体に適用されるデータ記録媒体に関する。
【０００２】
【従来の技術】コンピュータプログラムなどを記録する記録媒体として、フロッピーディスク等と称される磁気ディスクが広く使用されている。また、磁気ディスクよりも記録密度の高い媒体として、レーザビームを記録や再生に使用する光磁気ディスクや光ディスクも使用されている。
【０００３】これらのディスクにプログラムを記録させる場合には、例えば各ディスクのデータ記録トラックに設定されたセクタに、このディスクの記録フォーマットに従った順序でデータを記録し、再生するときには記録フォーマットに従ったセクタ順に記録データを再生させて、記録されたプログラムを得るようにしている。
【０００４】これに対し、ディスクに記録されたデータのセキュリティ性を高めるために、通常のフォーマットに従ったセクタ順にデータを記録させるのではなく、適当なオフセット等をセクタに付加して記録することが行われている。このようにしてディスクに記録されたデータを読出す場合には、セクタを変更させたオフセットデータ等が読出すコンピュータ側に用意されてないと、正しいプログラムを得ることができず、プログラムの不正使用を防止することができる。
【０００５】
【発明が解決しようとする課題】ところが、このようにセクタの順序を変更させた場合でも、ディスク１枚に記録されたデータを全てそのまま別のディスクに複製するコピー装置で複製することは可能である。従って、このようなコピー装置でオリジナルのディスクから複製を行い、複製されたディスクを使用するコンピュータ側に、データの正確な読出しに必要なセクタのオフセットデータ等が用意されていれば、プログラムを複製して不正使用することが可能である。従って、このような記録方法は、プログラムの不正使用防止の観点からは不完全な記録方法である。
【０００６】一方、記録するプログラムデータそのものを、所定の暗号方式に基づいて暗号化し、暗号化されたデータをディスクに記録する方法もある。この場合には、このプログラムデータを解読する暗号化プログラムが必要で、暗号化プログラムが記録されたディスクなどを別に用意する必要があが、この暗号化プログラムが記録されたディスクなどの管理が煩わしく、このディスクを紛失した場合にはプログラムデータの復号ができなくなってしまう。このような紛失による復号不可とならないようにするためには、暗号化プログラムが記録されたディスクをコピーしておくことが考えられるが、暗号化プログラムがコピーされると、それだけセキュリティ性が低くなり、暗号化した意味がなくなってしまう。
【０００７】また、このように暗号化する場合に、或るキーワードを使用してスクランブルを掛ける方法もあるが、このような場合には暗号化する側と復号化する側とで同一のキーワードを知っている必要があり、何回も同じキーワードを使用すると、キーワードが知れ渡って暗号化の意味がなくなってしまう。従って、使い捨てキーワード方式と称する使用するキーワードを逐次変更する方法もあるが、キーワードの管理が煩雑になってしまう。
【０００８】ここまでの説明では、ディスクにコンピュータプログラムデータを記録させる場合について説明したが、磁気テープなどの他の記録媒体にデータを記録させる場合にも、セキュリティ性についての同様な問題点がある。
【０００９】本発明の目的は、プログラムなどの各種データをディスク，テープ等の記録媒体に記録させる場合に、セキュリティ性が高く且つ使い勝手の良い記録ができるようにすることにある。
【００１０】

【課題を解決するための手段】本発明は、例えば図１に示すように、所定の方法でデータが記録される記録媒体１２を所定の筐体１１に収納させ、この筐体１１の所定箇所にメモリと演算手段とを有するＩＣ２０を取付けてなるデータ記録媒体において、記録媒体１２に起動プログラムと暗号化されたデータとを記録させ、暗号化されたデータの暗号化プログラムと暗証番号のデータとをＩＣ２０内のメモリに記憶させ、記録媒体１２に記録されたデータを読出す場合又は記録媒体１２にデータを書込む場合に、入力された暗証番号をＩＣ２０に供給させて、このＩＣ２０内のメモリに記憶された暗証番号と演算手段が照合させ、暗証番号が一致した場合には、ＩＣ２０内のメモリに記憶された暗号化プログラムに従って、記録媒体１２に記録された暗号化されたデータの復号又は記録媒体１２に記録するデータの暗号化をできるようにしたものである。

【００１１】またこの場合に、ＩＣ内での暗証番号の照合で、予め定めた所定回連続して不一致を検出したとき、以後の照合で暗証番号が一致しても暗号化プログラムを出力させないブロックを行うようにしたものである。

【００１２】さらに、このブロックされた状態で、上記暗証番号とは別に設定された暗証番号を入力させることで、ブロックの解除を行うようにしたものである。

【００１３】また、上述した場合に、ＩＣ内のメモリに付加情報を記憶させるようにしたものである。

【００１４】

【作用】本発明によれば、記録媒体に記録されたデータの暗号化プログラムが、この記録媒体を収納する筐体に取付けられたＩＣに記憶され、暗証番号が一致しない限りこのＩＣから暗号化プログラムを読出すことができなく、従って記録媒体に記録されたデータの復号もできなく、記録されたデータの不正使用を防止するセキュリティ性が高い。

【００１５】この場合、ＩＣ内での暗証番号の照合で、予め定めた所定回連続して不一致を検出したとき、以後の照合で暗証番号が一致しても暗号化プログラムを出力させないブロックを行うことで、不正な使用を防止する効果がより高くなる。

【００１６】また、このブロックされた状態で、暗号化プログラム読出し用の暗証番号とは別に設定された暗証番号を入力させることで、ブロックの解除を行うようにしたことで、ブロックされた状態の解除が良好にできる。

【００１７】さらに、ＩＣ内のメモリに付加情報を記憶させることで、暗号化プログラムが記憶されたＩＣが効率よく使用される。

【００１８】

【実施例】以下、本発明の実施例を、添付図面を参照して説明する。

【００１９】本例においては、フロッピーディスクと称される磁気ディスクを使用したコンピュータ用のデータ記録媒体に適用したもので、図１～図３に示すように構成する。図１は本例のフロッピーディスクの全体構成を示す図で、図中１０はフロッピーディスク全体を示し、このフロッピーディスク１０は、合成樹脂で形成された筐体１１の中に、直径３．５インチの磁気ディスク１２が収納され、開閉自在なシャッタ１３が取付けてある。このシャッタ１３には窓部１３ａが設けられ、シャッタ１３が開状態のとき、筐体１１側の開口部１１ａと窓部１３ａとの位置が一致して、磁気ディスク１２の信号記録面が露出する。

【００２０】そして、このフロッピーディスク１０を後述する駆動装置に装着させたとき、磁気ディスク１２が所定の駆動手段により回転すると共に、シャッタ１３が開状態になって露出した信号記録面に磁気ヘッドが近接し、このヘッドでデータの記録や再生ができる。なお、この信号記録面は、片面だけの場合と、両面に形成された場合とがある。ここまでは、通常のフロッピーディスクの構成である。

【００２１】そして本例においては、このフロッピーディスク１０の筐体１１の隅に、１チップのＩＣ（集積回路）２０が内蔵させてある。このＩＣ２０は、筐体１１の表面から見ると、図２に拡大して示すように、８個の接点２１，２２，２３，‥‥２８が露出しただけとしてあり、内部の回路は図３に断面で示すように筐体１１を構成する樹脂内に埋め込まれている。なお、ＩＣ２０の内部の構成は後述する。

【００２２】次に、このように構成されるフロッピーディスク１０の駆動装置の構成を説明する。図４及び図５は、この駆動装置の構成を示す図で、図中３０はフロッピーディスク駆動装置全体を示し、このフロッピーディスク駆動装置３０は、フロッピーディスク１０を装着するための窓部３１を有し、この窓部３１から内部に装着されたフロッピーディスク１０は、図５に断面で示すように、所定のチャッキング機構３３によりモータ３２側と接続され、モータ３２により所定速度に回転駆動される。そして、図示しない磁気ヘッドにより、記録や再生が行われ、後述するホストコンピュータ側から供給される記録データが磁気ディスク１２に記録されると共に、磁気ディスク１２より再生したデータがホストコンピュータ側に供給される。

【００２３】そして、フロッピーディスク１０の表面に露出した８個の接点２１～２８と接続するために、端子ユニット４０が設けられ、この端子ユニット４０に配された８個の接片４１，４２，４３，‥‥４８の先端が、それぞれ対応した接点２１～２８と接触するようにしてある。そして、各接片４１～４８は、ホストコンピュータ側の所定のインターフェースと接続させてあり、ホストコンピュータ側の制御で、記憶データの読出しなどの

処理ができるようにしてある。

【００２４】次に、本例のフロッピーディスク１０に内蔵されたＩＣ２０の構成を説明すると、図６に示すように、ここでは８個の接点２１～２８の内の６個の接点２１～２６が使用され、接点２１が電源端子ＶＣＣとされ、接点２２が内蔵されたＥＥＰＲＯＭ５５のプログラム電圧入力端子ＶＰＰとされ、接点２３がシリアルデータ入出力端子Ｉ／Ｏとされ、接点２４がクロック入力端子ＣＬＫとされ、接点２５がリセット信号入力端子ＲＳＴとされ、接点２６が接地端子ＧＮＤとされる。

【００２５】そして、ＩＣ２０の内部の回路として、演算処理を行う中央制御装置（ＣＰＵ）５１と、ＩＣ２０内と外部との間でデータ入出力を行うためのシリアル／パラレル変換回路５２と、このシリアル／パラレル変換５２に変換用クロックを供給するための分周器５３と、データを一時的に記憶するＲＡＭ５４と、暗証番号などの保存及び書き換えが必要なデータを記憶するＥＥＰＲＯＭ５５と、暗号化プログラムなどのプログラムを記憶するＲＯＭ５６とで構成され、中央制御装置５１とシリアル／パラレル変換回路５２と各メモリ５４，５５，５６との間はバスラインで接続されている。

【００２６】そして、中央制御装置５１と分周器５３には、接点２４（クロック入力端子ＣＬＫ）に得られるクロックが供給され、このクロックに基づいて中央制御装置５１が作動する。この場合、接点２５（リセットパルス入力端子ＲＳＴ）に所定のリセット信号が供給されることで、中央制御装置５１が起動される。また、分周器５３でクロックを分周した信号をシリアル／パラレル変換回路５２に供給し、この分周信号に基づいてシリアルデータからパラレルデータへの変換又はパラレルデータからシリアルデータへの変換を行う。そして、シリアル／パラレル変換回路５２には、外部との入出力端子としての接点２３（シリアルデータ入出力端子Ｉ／Ｏ）が接続され、外部から接点２３を介して供給されるシリアルデータをパラレルデータに変換し、バスラインを介して中央制御装置５１などに供給する。また、バスラインを介してシリアル／パラレル変換回路５２に供給されるパラレルデータを、シリアルデータに変換して、接点２３から外部のコンピュータ（ホストコンピュータ）側に供給する。

【００２７】また、このＩＣ２０のＥＥＰＲＯＭ５５に記憶されるデータは、外部から接点２２（プログラム電圧入力端子ＶＰＰ）に所定のプログラム電圧が供給されることで、書き換えが可能とされている。

【００２８】次に、このＩＣ２０が内蔵されたフロッピーディスク１０とアクセスされるホストコンピュータ側の構成を説明する。図７は、このホストコンピュータの構成を示す図で、図中６１はメインの中央制御装置（ＣＰＵ）を示し、この中央制御装置６１には、バスラインを介してフロッピーディスクインターフェース６２，ハードディスクユニット６３，ＲＡＭ６４，ＲＯＭ６５，キーボードインターフェース６６，ＣＲＴインターフェース６８，シリアル／パラレル変換回路６９が接続されている。そして、フロッピーディスクインターフェース６２は、上述したフロッピーディスク駆動装置３０に装着されたフロッピーディスク１０の磁気ディスク１２側の記録データと中央制御装置６１側とのインターフェースが行われると共に、フロッピーディスク１０に内蔵されたＩＣ２０と中央制御装置６１側とのインターフェースが行われる。

【００２９】また、キーボードインターフェース６６には、キーボード６７が接続させてあり、キーボード６７の操作情報がインターフェース６６を介して中央制御装置６１側に伝送される。また、ＣＲＴインターフェース６８には、ＣＲＴディスプレイ装置７０が接続され、バスラインを介して供給される表示データがＣＲＴディスプレイ装置７０側に供給されて、対応した文字や画像が表示される。さらに、シリアル／パラレル変換回路６９を介して接続された外部機器（プリンタ等の周辺機器：図示せず）に、データを伝送することができるようにしてある。

【００３０】そして、このように構成されたホストコンピュータと、フロッピーディスク１０内のＩＣ２０との間では、図９に示すような処理で通信が行われ、ＩＣ２０を使用したデータ処理が行われる。即ち、最初にホストコンピュータ側から電源ＶＣＣとプログラム電圧ＶＰＰとして所定の電位の信号を供給すると共に、所定の周波数のクロックＣＬＫを供給して、ＩＣ２０が作動できる状態を設定する（ステップ２０１）。また、この最初の状態ではローレベル“Ｌ”のリセット信号を供給し、ＩＣ２０内の中央制御装置５１をリセットされた状態にする。

【００３１】そして、リセットパルスＲＳＴをハイレベル“Ｈ”に変化させてリセットを解除し、ＩＣ２０を起動させる（ステップ２０２）。ここで、ＩＣ２０が起動したときには、ＩＣ２０内の中央制御装置５１からホストコンピュータ側に、応答信号としてデータ交換に必要な初期データが転送される（ステップ２０３）。この初期データには、ＩＣ２０が受け取るデータの論理レベルやファーストビットなどを決定する情報などが含まれている。

【００３２】そして、ホストコンピュータの中央制御装置６１側では、この初期データを受信すると、ＩＣ２０とのインターフェースを対応した状態に設定し、以後のセッションを行う。次に、ホストコンピュータからは、コマンドをＩＣ２０内の中央制御装置５１に伝送させる（ステップ２０４）。このコマンドは、例えば5バイトで構成され、命令体系の属性，命令，パラメータ等を示す。

【００３３】そして、ＩＣ２０の中央制御装置５１で

は、伝送されたコマンドが、このＩＣＩに与えられた命令体系に属し、なお且つ命令やパラメータが正しいか否か判断し、判断した結果しての認証データをホストコンピュータに返送する（ステップ２０５）。また、コマンドが正常と判断する認証データを返送した場合には、続いてコマンドに対応したデータを転送させる（ステップ２０６）。このデータの転送方向は、コマンドにより設定される。なお、コマンドによってはデータの転送がない場合もある。

【００３４】そして最後に、ＩＣ２０側の処理が終了したことを示すステータスをホストコンピュータ側に送信し（ステップ２０７）、このセッションを終了する。その後、ホストコンピュータは必要に応じてステップ２０４のコマンド送信からステップ２０７のステータス受信までを繰り返す。

【００３５】そして、本例においてはこの場合に使用されるコマンドとして、２つの体系のコマンドが用意されている。即ち、第１のコマンドとして管理コマンドが用意され、利用者に知られることなく扱われるコマンドで、フロッピーディスク１０の発行者と管理者だけに使用が許可されたコマンドである。

【００３６】そして、第２のコマンドがＩＣ２０とのインターフェースを制御するコマンドで、このコマンドを使用してフロッピーディスク１０を使用する際のアクセスが行われる。

【００３７】以上説明した構成にて本例のＩＣ内蔵のフロッピーディスク１０が使用されるが、以下この内蔵されたＩＣ２０を使用する場合の処理の一例を、図８のフローチャートを参照して説明する。

【００３８】ここでは、フロッピーディスク１０内の磁気ディスク１２に、コンピュータ用プログラムデータを暗号化して記録させ、ＩＣ２０内のＲＯＭ５６に、その暗号化プログラムを記憶させておく。また、磁気ディスク１２には、記録されたプログラムデータを読出すのに必要な起動プログラムを記録させておく。この起動プログラムは暗号化させない。そして、ＩＣ２０から暗号化プログラムを読出すための暗証番号（所定桁の数字による番号）を、ＩＣ２０に設定できるようにし、この設定された暗証番号のデータをＩＣ２０内のＥＥＰＲＯＭ５５に保存させておく。また、この暗号化プログラム読出し用の暗証番号とは別に、後述するブロック解除用の暗証番号も設定してＩＣ２０内のＥＥＰＲＯＭ５５に保存させておく。

【００３９】そして、ＩＣ２０内に記憶された暗号化プログラムは、ＥＥＰＲＯＭ５５に登録された暗証番号と同じ番号がホストコンピュータ側から供給された場合だけ、ホストコンピュータ側に読出せるようにしてある。また、登録された暗証番号とは異なる番号が入力された場合には、この誤った暗証番号の入力処理が３回連続して行われたとき、ＩＣ２０内の中央制御装置５１の制御で、このＩＣ２０からの暗号化プログラムの読出しを禁止するブロック処理を行うようにしてある。このブロックされた状態では、正しい暗証番号が入力されても、暗号化プログラムの読出しを禁止する。

【００４０】そして、このブロックされた状態で、ＥＥＰＲＯＭ５５に登録されたブロック解除用の暗証番号と同じ番号がホストコンピュータ側から供給されたときには、ブロックを解除するようにしてある。但し、このブロック解除用の暗証番号の入力を１０回連続して誤ったときには、ＩＣ２０内の中央制御装置５１が、ブロック解除用の暗証番号の入力自体を受け付けないようにして、よりレベルの高いブロックが行われるようにしてある。このレベルの高いブロックが行われた状態では、このセキュリィティシステムの管理者（フロッピーディスクの発行元）が、管理用のツールを使用して解除しない限り、ＩＣ２０とアクセスできる状態に復帰しないようにしてある。

【００４１】また、磁気ディスク１２に暗号化されて記録されたプログラムに関する暗号化する必要のない付加情報（簡単な目次，日付，利用者名などの任意の情報）を、ＩＣ２０内のメモリ（ＲＡＭ５４など）に記憶できるようにしてある。

【００４２】このように暗号化されてフロッピーディスク１０内の磁気ディスク１２に記録されたデータを再生（又は磁気ディスク１２に暗号化してデータを記録）する場合の処理を、以下図８のフローチャートに従って順に説明する。まず、ホストコンピュータは磁気ディスク１２に記録された起動プログラムを読出して、ホストコンピュータ内に読み込ませる（ステップ１０１）。この動作は、従来のフロッピーディスクに記録されているプログラムの起動時の動作と同じである。

【００４３】そしてこの起動後には、ホストコンピュータ側のＣＲＴディスプレイ装置７０に、暗証番号の入力要求があることを表示させる（ステップ１０２）。この表示の後、キーボード６７で暗証番号の入力操作が行われると、この入力された番号のデータをフロッピーディスク１０内のＩＣ２０に転送させる（ステップ１０３）。そして、ホストコンピュータ側でＩＣ２０からのステータスを受信すると（ステップ１０４）、このとき受信したデータでＩＣ２０がブロックされているか否か判断する（ステップ１０５）。

【００４４】このとき、ブロックされているときには、ホストコンピュータ側のＣＲＴディスプレイ装置７０に、ブロックされていることを表示させる（ステップ１０６）。また、ブロックされていない場合には、暗証番号が一致するか否かの認証結果の判断を行い（ステップ１０７）、暗証場合が一致した場合には、キーボード６７の操作などでモード入力を行う（ステップ１０９）。このモード入力は、ＩＣ２０に記憶された付加情報の読出しを行うか、或いは暗号化プログラムの読出しを行う

かを選択するためのものである。

【００４５】また、ステップ１０７で暗証番号が一致しなかった場合には、ホストコンピュータ側のＣＲＴディスプレイ装置７０に、暗証番号の再入力を要求する表示をさせた後（ステップ１０９）、ステップ１０３に戻る。

【００４６】そして、ステップ１０９でモード入力が行われた後は、ホストコンピュータ側の中央制御装置６１が、入力されたモードが付加情報を確認するものであるのか否か判断する（ステップ１１０）。ここで、付加情報を確認するモードでない場合には、ＩＣ２０内のＲＯＭ５６に記憶された暗号化プログラムを、ホストコンピュータ側のＲＡＭ６４に転送させる処理を行う（ステップ１１１）。そして、このとき必要とする処理が、データをフロッピーディスクに記録させる処理（書込ませる処理）であるのか否か判断し（ステップ１１２）、記録させる場合には、ＲＡＭ６４に転送された暗号化プログラムに基づいたホストコンピュータ側の処理で、記録するデータを暗号化されたデータとし、この暗号化されたデータを磁気ディスク１２の所定セクタに記録させる（ステップ１１３）。また、このときに生じる付加情報（記録日時などのデータ）を、ＩＣ２０に転送させて、付加情報を記憶するエリアに記憶させておく（ステップ１１４）。

【００４７】そして、ステップ１１２で再生させる処理（読出させる処理）であると判断したときには、磁気ディスク１２に記録された所定のデータを再生してホストコンピュータ側に転送させ、ＲＡＭ６４に転送された暗号化プログラムに基づいたホストコンピュータ側の処理で、再生されたデータの復号化を行い、この復号化されたデータを指定されたドライブ（ハードディスク又は他のフロッピーディスクなど）側に供給させて書込ませておく（ステップ１１５）。

【００４８】そして、この記録や再生の処理が終了した後は、ホストコンピュータ側のＲＡＭ６４が記憶している暗号化プログラムを消去させるパージ処理を行う（ステップ１１６）。この暗号化プログラムの消去処理が終了すると、このときに必要なＩＣ２０のセッションが終了したか否か判断し（ステップ１１７）、終了したときには、ホストコンピュータ側のＤＯＳ（ディスクオペレーティングシステム）を使用した処理に戻る（ステップ１１８）。

【００４９】また、ステップ１１０で付加情報を確認するモードである場合には、ＩＣ２０に記憶された付加情報をホストコンピュータ側に読込ませ（ステップ１１９）、この読込んだ付加情報をＣＲＴディスプレイ装置７０に表示させる（ステップ１２０）。そして、この表示を行うとステップ１１７に移る。

【００５０】そして、ステップ１１７でＩＣ２０のセッションが終了してないと判断したときには、ステップ１０８に戻り、モード入力処理から再度実行させる。

【００５１】ステップ１０６でブロックされていることを表示した後には、キーボード６７でブロック解除用暗証番号の入力操作があるか否か判断し（ステップ１２１）、この入力操作がある場合には、この入力されたブロック解除用暗証番号のデータをＩＣ２０へ転送させる（ステップ１２２）。そして、ホストコンピュータ側でＩＣ２０からのステータスを受信すると（ステップ１２３）、ブロック解除用暗証番号が一致したか否かの認証処理を行い、一致したか否か判断する（ステップ１２４）。ここで、一致した場合には、ステップ１０８に移って、モード入力を受け付ける。また、一致しなかった場合には、ＩＣ２０とのアクセスを終了して、ステップ１１８に移ってホストコンピュータ側のＤＯＳを使用した処理に戻る。

【００５２】以上のようにしてフロッピーディスク１０を使用して、暗号化されたデータの記録・再生が行われることで、暗号化されて記録されたデータの不正使用を効果的に防止できる。即ち、暗号化する方法に関するプログラムは、フロッピーディスク１０に内蔵されたＩＣ２０に記憶され、ディスクに記録や再生を行う場合で且つ暗証番号を知っている場合にだけ、この暗号化プログラムを読出してデータの暗号化や復号化が出来るようになっている。このため、暗証番号を知らない限り、記録されたデータを復号して読出すことができなく、不正使用の防止効果が高いと共に、暗号化プログラムを読出してコピーすることが困難で、暗号化プログラムが外部に漏れる可能性が少ない。

【００５３】従って、例えば１枚のフロッピーディスクに記録されたデータを、そのまま全てコピーする装置を使用して複製しても、暗号化プログラム自体は複製されず、フロッピーディスクに記録されたプログラムデータが不正使用されることが防止される。

【００５４】また本例の場合には、記録されたプログラムデータを読出すのに必要な起動プログラムを、暗号化せずに磁気ディスク１２に記録するようにしたので、ホストコンピュータからの制御でこの起動プログラムを読出すまでの動作は、従来のフロッピーディスクと同じであり、この起動プログラムに従って暗号化プログラムを読出す処理が行われるようにすれば、ホストコンピュータ側では暗号化や復号化のために特別な制御プログラムを用意しておく必要がなく、従来のフロッピーディスクを使用する場合と同様なプログラム構成の制御で実現できる。

【００５５】また、本例のように１枚のフロッピーディスクにＩＣ２０を内蔵させた場合には、ディスクと暗号化プログラムとが１対１で対応しているので、１枚のフロッピーディスク毎に暗号化プログラムを変えることができる。このように１枚のフロッピーディスク毎に暗号化プログラムを変えることで、例え何れかの暗号化プロ

グラムが外部に漏れても、この暗号化プログラムに対応した特定のディスクのデータだけが解読できるだけで、このシステムが適用されるディスクの記録データ全てが解読できるものではなく、不正使用防止効果がより高くなる。

【００５６】また、本例の場合には、暗証番号の照合処理を複数回（上述実施例では３回）連続して誤って行ったとき、不正に暗号化プログラムを読出そうとしている可能性が高いとして、内蔵されたＩＣからの暗号化プログラムの読出しをブロックするようにしたので、暗証番号を知らない者が何回も照合作業を行って暗証番号を解読する作業ができないようにしてあり、この点からも不正使用の防止効果が高い。

【００５７】さらに、この内蔵されたＩＣからの暗号化プログラムの読出しがブロックされた状態で、このブロック状態を解除することが別の暗証番号でできるようにしてあるので、万一ブロックされたときの対処が容易にできると共に、このブロック状態を解除するための暗証番号の照合作業でも、複数回（上述実施例では１０回）連続して誤って行ったときには、内蔵されたＩＣからの暗号化プログラムの読出しを完全にブロックするようにしたので、さらに不正使用の防止に対する効果が高い。

【００５８】なお、上述実施例ではフロッピーディスクへの記録・再生を行う場合に、ＩＣ２０からホストコンピュータ側に暗号化プログラムを転送させて、ホストコンピュータ内で暗号化や復号化の処理を行うようにしたが、ＩＣ２０からの暗号化プログラムの読出しは出来ないようにして、代わりにディスクから再生したデータの復号化やディスクに記録するデータの暗号化を、ＩＣ２０内の処理で行うようにしても良い。この場合には、暗号化プログラムが全く外部に転送されないので、ホストコンピュータ側で暗号化プログラムがコピーされる可能性が全くなく、セキュリティ性が非常に高い。但し、ディスクから再生したデータやディスクに記録するデータを、一旦ＩＣ２０に転送させて処理させる必要があり、ホストコンピュータ側で処理する場合に比べて、データの再生や記録に若干時間がかかる。

【００５９】また、上述実施例では暗号化方法については特に説明しなかったが、コンピュータ用データに適用できる各種暗号化方法が使用できる。例えば、フロッピーディスクの１セクタに相当するバイト数毎に暗号化する方法，１トラックに相当するバイト数毎に暗号化する方法，データやプログラムを一括して暗号化する方法などが考えられる。また、所定のセクタやトラック毎に暗号化する場合に、この暗号化する単位データ毎に暗号化アルゴリズムを変更するようにしても良い。また、１枚のフロッピーディスクに記録するデータの内の一部のデータだけを暗号化するようにしても良い。

【００６０】また、上述実施例ではディスクに記録されるデータの付加情報をＩＣ２０に記憶させるようにしたが、この付加情報についても必要により暗号化して記憶させるようにしても良い。また、ＩＣ２０に記憶させる代わりに、磁気ディスク１２の所定のエリアに記録させるようにしても良い。

【００６１】さらに、上述実施例においては磁気ディスクに適用したが、他の記録媒体にも適用できることは勿論である。例えば、光磁気ディスク，光ディスクなどのディスク状の記録媒体や、磁気テープ等のテープ状の記録媒体にも適用できる。何れの場合でも、記録媒体を収納する筐体にＩＣを内蔵させれば対処できる。また、記録媒体に記録するデータについても、コンピュータ用のプログラム以外の各種データが適用できる。

【００６２】

【発明の効果】本発明によると、記録媒体に記録されたデータの暗号化プログラムが、この記録媒体を収納する筐体に取付けられたＩＣに記憶され、暗証番号が一致しない限りこのＩＣから暗号化プログラムを読出すことができなく、従って記録媒体に記録されたデータの復号もできなく、記録されたデータの不正使用を防止するセキュリティ性が高い。例えば、暗証番号を知らない使用者が記録媒体に記録されたデータを別の記録媒体にコピーしても、暗号化されたままでコピーされ、コピーされたデータを復号する暗号化プログラムはコピーされず、コピーされたデータを復号することは困難で、不正使用が防止される。

【００６３】この場合、ＩＣ内での暗証番号の照合で、予め定めた所定回連続して不一致を検出したとき、以後の照合で暗証番号が一致しても暗号化プログラムを出力させないブロックを行うことで、不正な使用を防止する効果がより高くなる。

【００６４】また、このブロックされた状態で、暗号化プログラム読出し用の暗証番号とは別に設定された暗証番号を入力させることで、ブロックの解除を行うようにしたことで、ブロックされた状態の解除が良好にできる。

【００６５】さらに、ＩＣ内のメモリに付加情報を記憶させることで、暗号化プログラムが記憶されたＩＣが効率よく使用される。

【図面の簡単な説明】

【図１】本発明の一実施例を示す斜視図である。

【図２】一実施例の要部を示す平面図である。

【図３】図２の III-III線に沿う断面図である。

【図４】一実施例のディスクが適用されるディスク駆動装置の構成を示す平面図である。

【図５】図４のＶ－Ｖ線に沿う断面図である。

【図６】一実施例の内蔵ＩＣを示す構成図である。

【図７】一実施例の内蔵ＩＣと接続されるホストコンピュータの一例を示す構成図である。

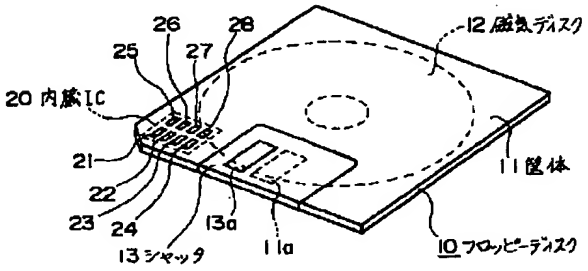
【図８】一実施例のディスク書込み，読出し処理を示すフローチャート図である。

【図９】一実施例の内蔵ＩＣとホストコンピュータとの通信状態を示す説明図である。

【符号の説明】

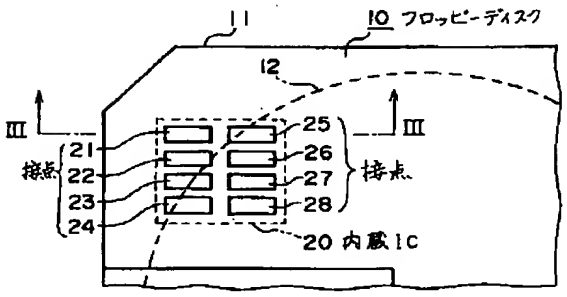
１０　フロッピーディスク
１１　筐体
１２　磁気ディスク
１３　シャッタ
２０　内蔵ＩＣ
２１，２２，２３，２４，２５，２６，２７，２８　接点
３０　フロッピーディスク駆動装置
４０　端子ユニット
４１，４２，４３，４４，４５，４６，４７，４８　接片
５１　中央制御装置（ＣＰＵ）
５６　ＲＯＭ

【図１】



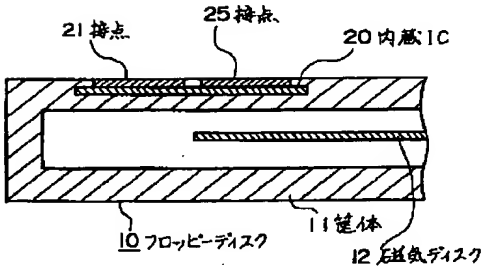
フロッピーディスクの構成

【図２】



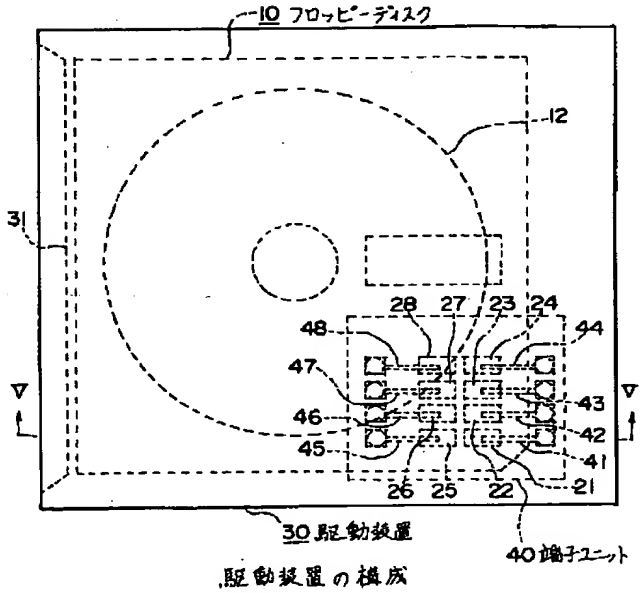
要部の平面図

【図３】



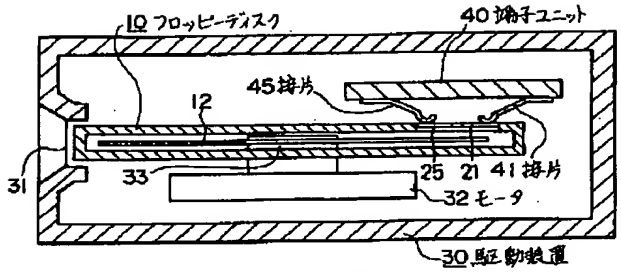
III-III線に沿う断面図

【図４】



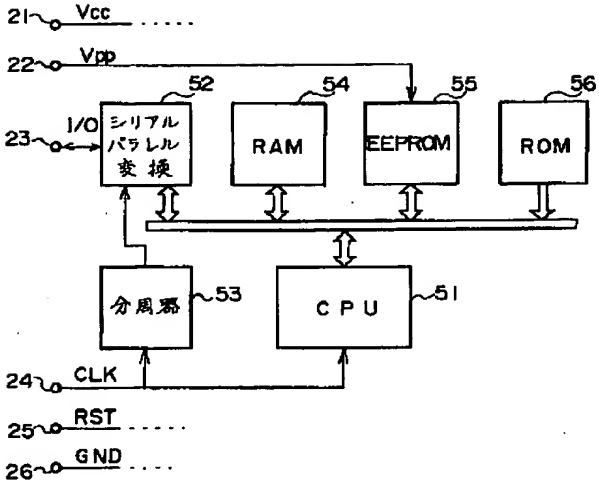
駆動装置の構成

【図５】



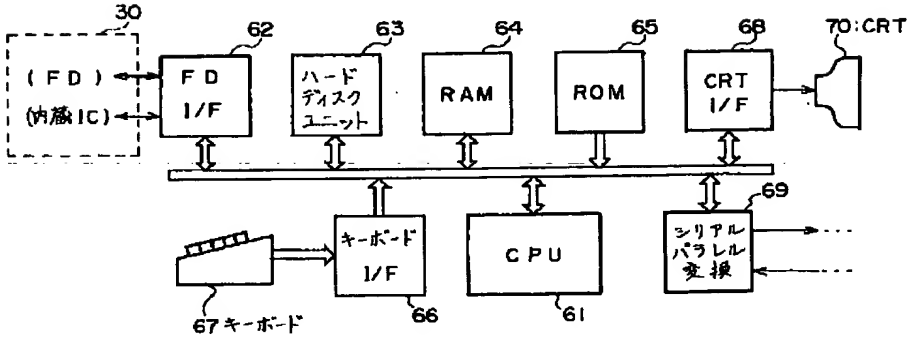
Ⅴ－Ⅴ 線に沿う 断面図

【図６】



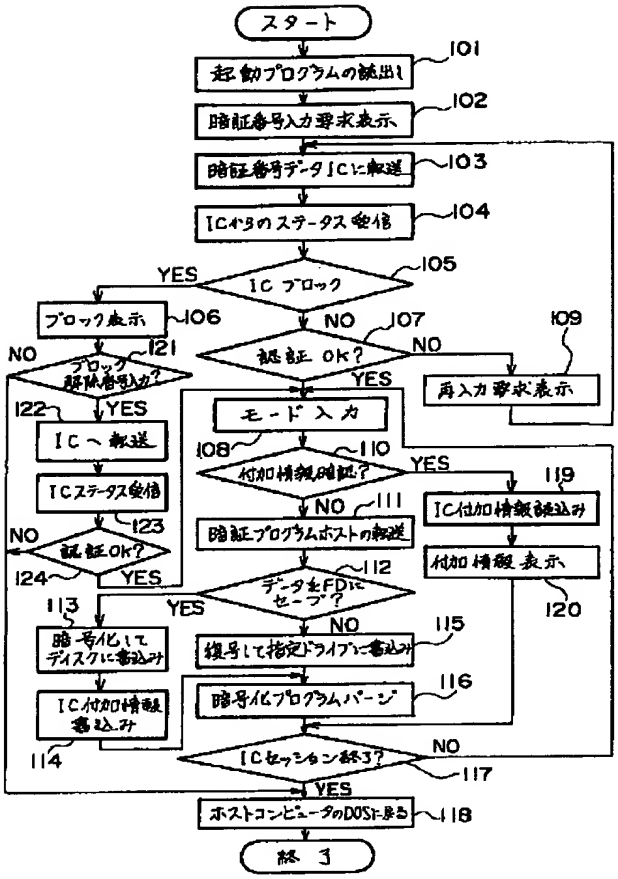
内蔵ＩＣの構成

【図７】



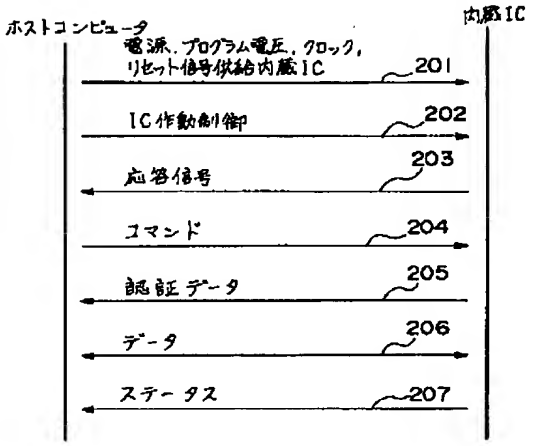
ホストコンピュータの構成

【図８】



ディスクオうの読出・書込みの処理

【図９】



ホストコンピュータと内蔵ICとの通信状態